Think encrypted traffic is safe?

Think again.

There are a variety of reasons why companies don’t—or can’t—inspect all their SSL-encrypted traffic. But as SSL traffic increases, so do the threats.

If you’re not inspecting all SSL traffic, here is what you are missing...

80 percent

of all traffic on the Zscaler™ cloud is encrypted— an increase of 10% over the prior year

1.7 billion

SSL threats blocked by the Zscaler cloud in the past six months

400 percent

growth in phishing attacks delivered over SSL compared to 2017

2.7 million

phishing attacks over encrypted channels blocked by the Zscaler cloud per month

! **With sophisticated attackers, it’s getting difficult to distinguish a phishing site from a real one. The once-trusty green padlock no longer guarantees security.**

Most Phished Brands

Cybercriminals use well-known brands in their phishing attempts.

58% Microsoft

12% Facebook

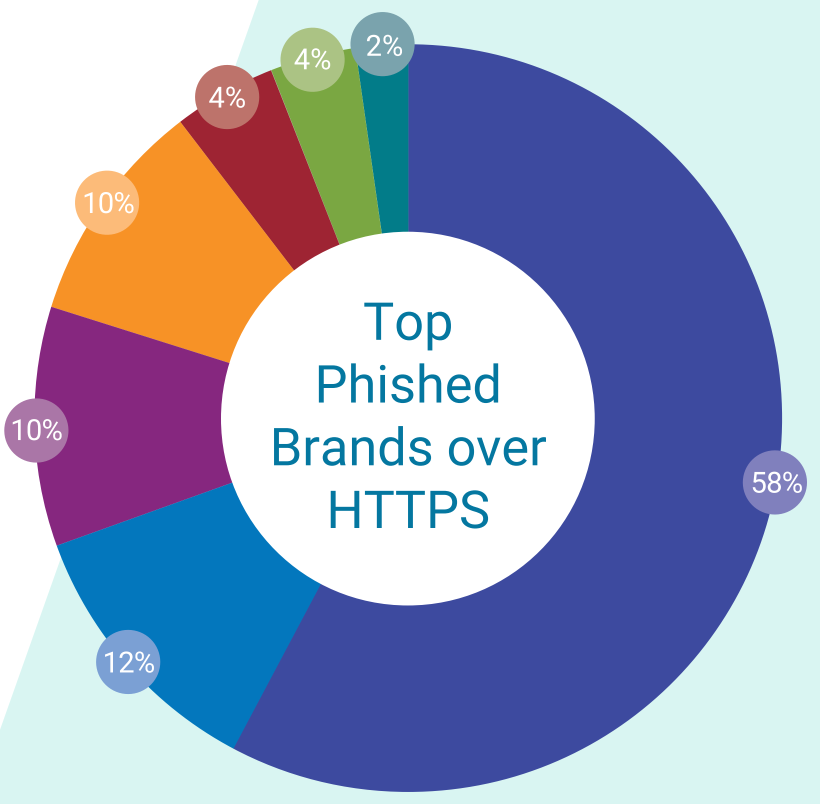
10% Amazon

10% Apple

4% Adobe

4% Dropbox

2% DocuSign



Botnet Threats

An average of **32 million** botnet callback attempts hidden in SSL traffic were blocked every month in 2018. The top five botnet families were:

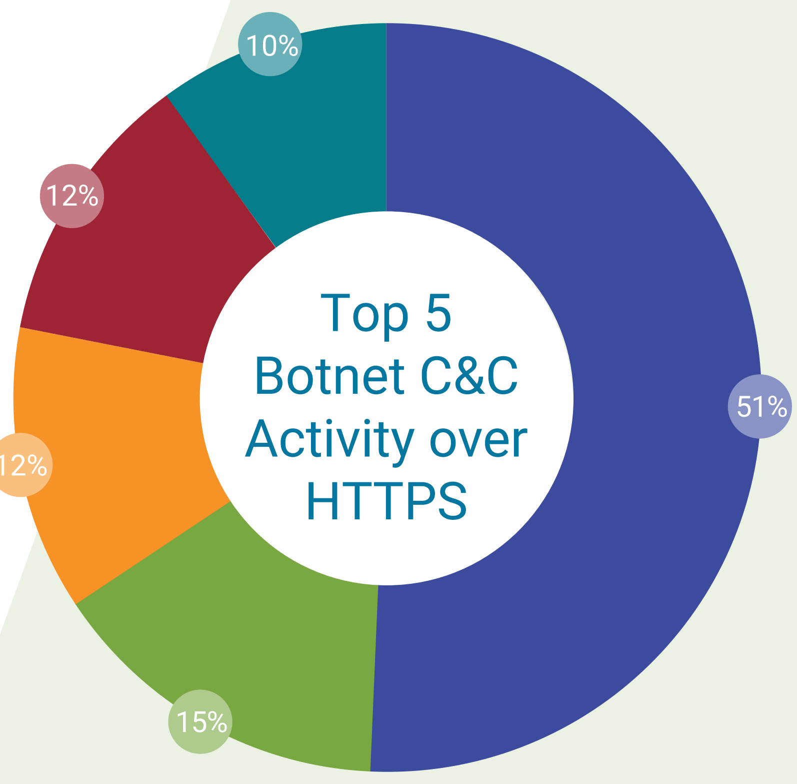
58% Trickbot

15% Emotet/Heodo/Feodo variants

12% Qadars

12% Dridex

10% Zbot variants



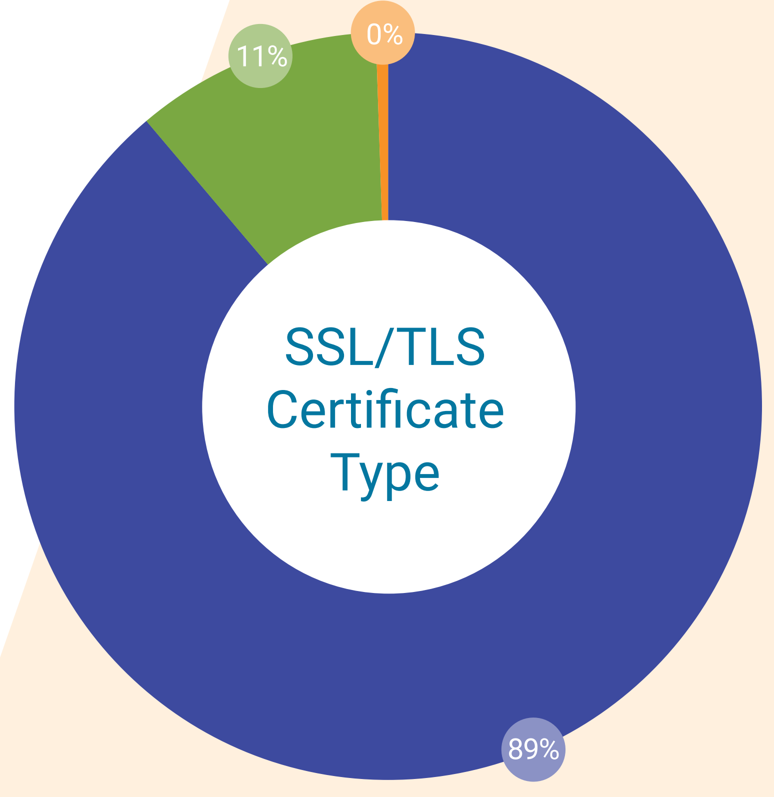
! **Cybercriminals are using encryption to conceal and launch attacks, as SSL certificates are now readily available at no charge. Allowing SSL traffic to go uninspected is riskier than ever.**

Types of Digital Certificates

Domain Validated (DV) certificates require minimal verification, as opposed to Organization Validated (OV) and Extended Validation (EV) certificates.

89% of blocked content used DV certificates.

11% of blocked content used OV certificates.



! **Cybercriminals continually create new attack vectors in an attempt to make money. Is your network robust enough to block these threats?**

Want to see more?

Download the Full Report

zscaler™